REMARKS

Applicant has reviewed and considered the Office Action mailed on May 2, 2007, and the references cited therewith. Claims 1, 3, 10, 20, 24, and 26 are amended, claims 2, 5, 7, 11-19, 21, 22, and 25 are canceled, and claims 27-29 are added; as a result, claims 1, 3, 4, 6, 8-10, 20, 23, 24, and 26-29 are now pending in this application.

35 USC § 112 Rejection of the Claims

Claim 15 was rejected under 35 USC § 112, first paragraph. Claim 15 has been canceled rendering this rejection moot.

35 USC §102 Rejection of the Claims

Claims 1-6, 8-10, & 13-19 were rejected under 35 USC § 102(e) as being anticipated by Sibert (U.S. Patent No. 7124170 B1). Claims 2, 5, and 13-19 have been canceled, rendering this rejection moot with respect to those claims. Independent claims 1 and 10 have been amended, and applicant believes this rejection with respect to those claims has been overcome as a result.

Applicant respectfully submits that Sibert does not disclose, teach, or suggest "a translation look-aside buffer (TLB), wherein the security enforcement mechanism allows a page table access in secure memory while the processor remains in a non-secure mode after a TLB miss in a non-secure process" as recited in claim 1 as amended. Further, applicant respectfully submits that Sibert does not disclose, teach, or suggest "wherein the hardware generated memory accesses are the result of a translation look-aside buffer (TLB) miss that occurs when the processor is running in a non-secure mode, and wherein the secure memory access occurs without the processor leaving the non-secure mode" as recited in claim 10 as amended.

Accordingly, applicants believe claims 1 and 10 are in condition for allowance. Further, applicants believe claims 3, 4, 6, 8, and 9 are in condition for allowance at least by virtue of dependency on claim 1.

35 USC §103 Rejection of the Claims

Claims 7, 11, & 12 were rejected under 35 USC § 103(a) as being unpatentable over Sibert (U.S. Patent No. 7124170 B1) in view of Mahon et al. (U.S. Patent No. 4809160 A). Claims 7, 11, and 12 have been canceled. Claim 1 has been amended to include the limitations of claim 7 and additional limitations. Claim 10 has been amended to include the limitations of claim 11 and additional limitations. This rejection is discussed with reference to independent claims 1 and 10 as amended. Applicant believes this rejection has been overcome by amendment, and further believes that claims 1 and 10 define over the combination of Sibert and Mahon.

As outlined in item 6 on page 10 of the office action, Mahon discloses "the target register 70 as shown in FIG. 3 contains the return address in Address Location 300 with the original, lower privilege level stored in two lower order bits 310. The TLB 30 then checks the access rights of the calling instruction as will be described shortly to determine if execute access is permitted" [column 3 lines 41-46]. Mahon also discloses "the gateway instruction resaves the actual privilege level of the calling routing ... and raises the privilege level of the calling routine to the privilege level specified within the page type field 412 of the TLB entry" [column 3 lines 52-57]. Accordingly, Mahon contemplates raising a privilege level of the calling routine (process) based on the contents of the TLB entry. Applicant notes that Mahon does not disclose what happens if a TLB miss occurs.

Independent claim 1 has been amended to include "a translation look-aside buffer (TLB), wherein the security enforcement mechanism allows a page table access in secure memory while the processor remains in a non-secure mode after a TLB miss in a non-secure process." Applicant respectfully submits that Mahon does not describe a TLB miss, nor does Mahon describe "a page table access in secure memory while the processor remains in a non-secure mode" as claimed. Further, applicant respectfully submits that the subject matter of claim 1 as amended is not disclosed, taught, or suggested by the combination of Sibert and Mahon.

Independent claim 10 has been amended to include "wherein the hardware generated memory accesses are the result of a translation look-aside buffer (TLB) miss that occurs when the processor is running in a non-secure mode, and wherein the secure memory access occurs without the processor leaving the non-secure mode." Applicant respectfully submits that Mahon

does not describe a TLB miss, nor does Mahon describe "wherein the secure memory access occurs without the processor leaving the non-secure mode" as claimed. Further, applicant respectfully submits that the subject matter of claim 10 as amended is not disclosed, taught, or suggested by the combination of Sibert and Mahon.

Claims 20-23 were rejected under 35 USC § 103(a) as being unpatentable over Mahon et al. (U.S. Patent No. 4809160 A) in view of Sibert (U.S. Patent No. 7124170 B1). Claims 21 and 22 have been canceled rendering this rejection moot with respect to those claims. Claim 20 has been amended in a manner similar to claims 1 and 10. Applicant respectfully submits that the combination of Mahon and Sibert does not disclose, teach, or suggest the subject matter of independent claim 20 as amended, including for example, "a translation look-aside buffer (TLB) miss has occurred in a non-secure process running in a processor's non-secure mode" and "performing a page table walk in secure memory without leaving the non-secure mode." Accordingly, applicants believe claim 20 is in condition for allowance. Applicant further believes claim 23 is in condition for allowance at least by virtue of dependency.

Claims 24-26 were rejected under 35 USC § 103(a) as being unpatentable over Mel et al. ("Tablet: Personal Computer of the Year 2000") in view of Sibert (U.S. Patent No. 7124170 B1). Claim 24 has been amended similar to claim 1, and is believed to be in condition for allowance for the reasons stated above. Claim 25 has been canceled, and claim 26 is believed to be in condition for allowance at least by virtue of dependency.

New Claims

Claims 27-29 have been added. Applicant respectfully submits that the cited references do not disclose, teach or suggest the subject matter of independent claim 27, including for example, "a security enforcement mechanism that allows access to page tables in secure memory when a translation look-aside buffer (TLB) miss occurs in the user non-secure mode, wherein the access to the page table occurs without the processor leaving the user non-secure mode". Accordingly, applicant believes claims 27-29 are in condition for allowance.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (952-473-8800) to facilitate prosecution of this application.

Respectfully submitted,

DENNIS M. O'CONNOR

By his Representatives,

Customer Number: 45445

Telephone Number: 952-473-8800

Date July 31, 2007 By Dana B. LeMoine

Dana B. LeMoine
Reg. No. 40,062

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 31 day of JULY 2007.

Kyrstin Ryan
Name

Kyrstin Ryan
Signature

IN THE DRAWINGS

Six replacement sheets of formalized drawings are included herewith.